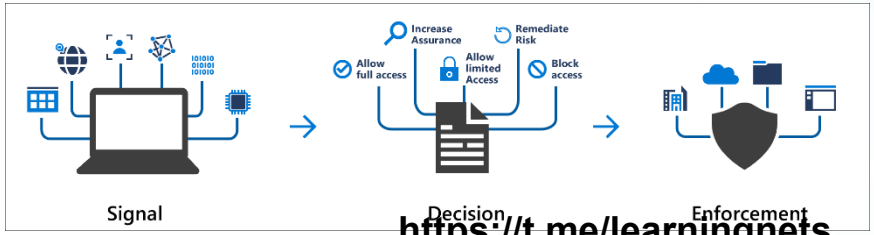
Conditional Access

examlabpractice.com

SOURCE: https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

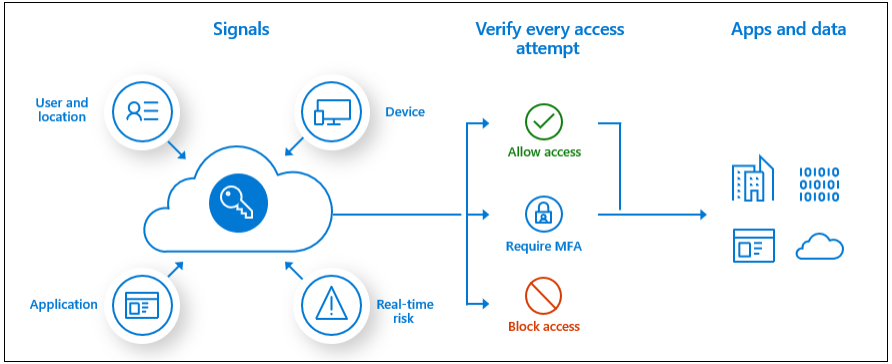
What is Conditional Access?

- Conditional Access is a tool in Azure that brings signals together for access decision making
- Signals help in decision making on whether to allow access or enforce certain policies



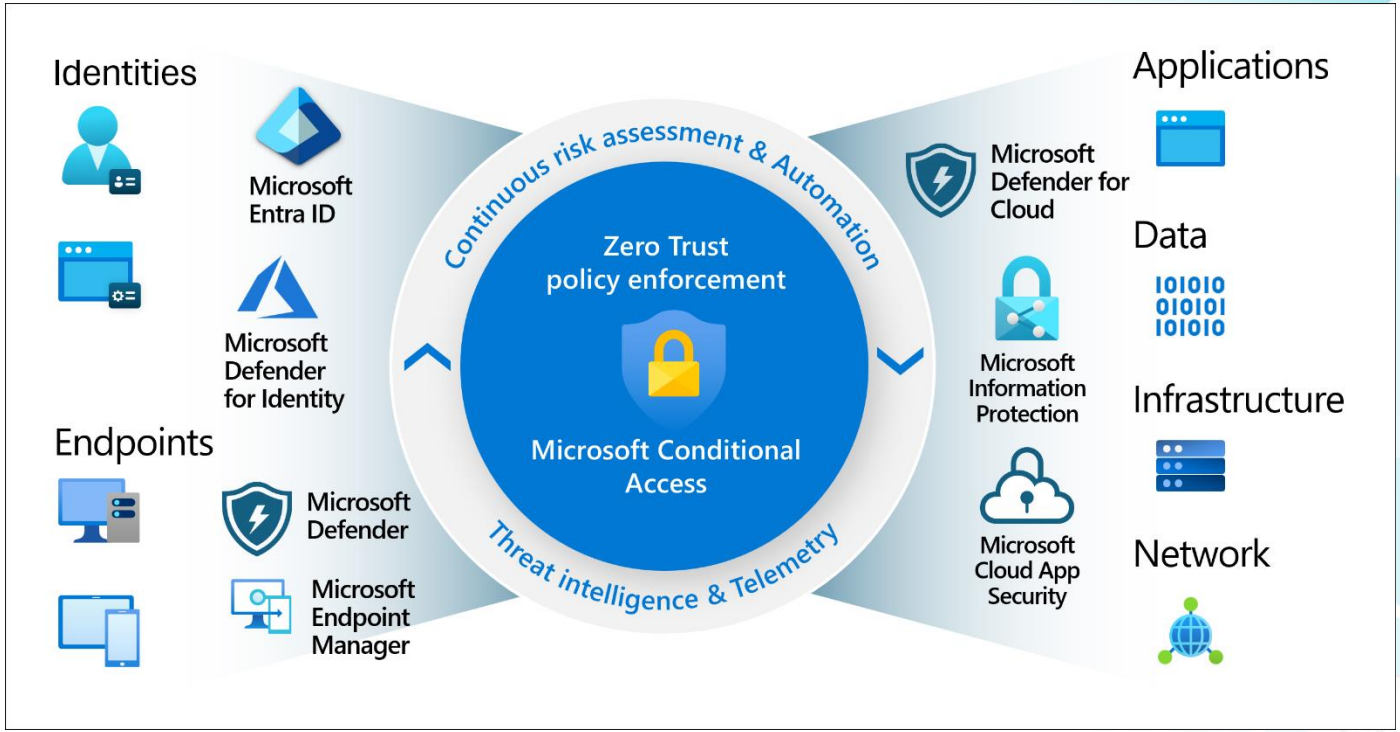
The Dilemma of Modern Administration

- Administrators today must allow users to be productive anywhere at anytime, and from a massive selection of applications
- Administrators are also expected to protect organizational data/assets all at the same time



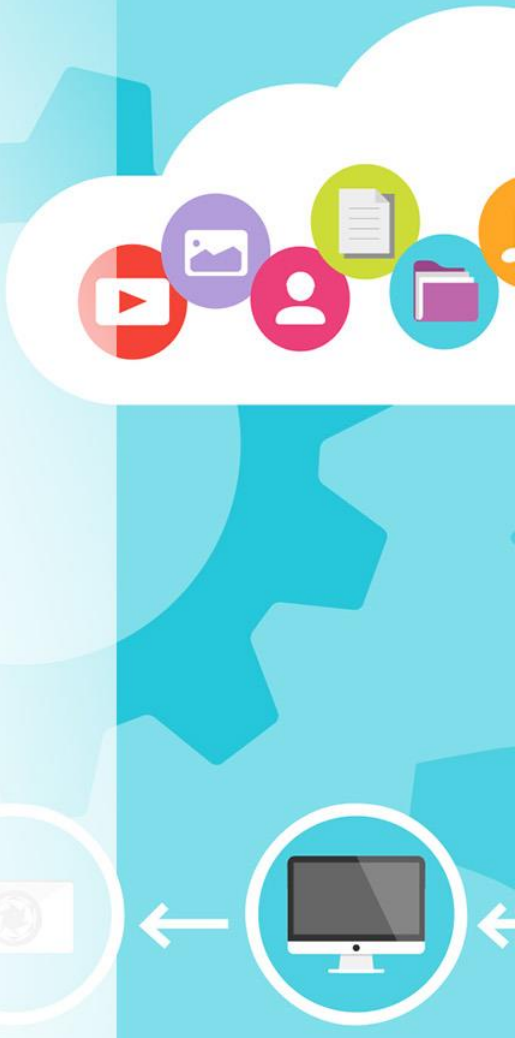
Common Signals

Conditional Access takes signals from various sources into account when making access decisions.



Signal Examples

- **User or group membership**
  - Policies can be targeted to specific users and groups giving administrators fine-grained control over access.
- **IP Location information**
  - Organizations can create trusted IP address ranges that can be used when making policy decisions.
  - Administrators can specify entire countries/regions IP ranges to block or allow traffic from.
- **Device**
  - Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.
  - Use filters for devices to target policies to specific devices like privileged access workstations.
- **Application**
  - Users attempting to access specific applications can trigger different Conditional Access policies.
- **Real-time and calculated risk detection**
  - Signals integration with Microsoft Entra ID Protection allows Conditional Access policies to identify and remediate risky users and sign-in behavior.
- **Microsoft Defender for Cloud Apps**
  - Enables user application access and sessions to be monitored and controlled in real time. This integration increases visibility and control over access to and activities done within your cloud environment.



Common Decisions

- **Block access**
  - Most restrictive decision
- **Grant access**
  - Less restrictive decision, can require one or more of the following options:
    - Require multifactor authentication
    - Require authentication strength
    - Require device to be marked as compliant
    - Require Microsoft Entra hybrid joined device
    - Require approved client app
    - Require app protection policy
    - Require password change
    - Require terms of use